

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
24 juillet 2003 (24.07.2003)

PCT

(10) Numéro de publication internationale
WO 03/060841 A1

(51) Classification internationale des brevets⁷ : G07F 7/10

(21) Numéro de la demande internationale :
PCT/FR03/00112

(22) Date de dépôt international :
15 janvier 2003 (15.01.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/00569 17 janvier 2002 (17.01.2002) FR

(71) Déposant (pour tous les États désignés sauf US) :
FRANCE TELECOM [FR/FR]; 6, place d'Alleray,
F-75015 Paris (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : CANARD,
Sébastien [FR/FR]; 4, résidence Olympia, F-14000 Caen
(FR). GIRAULT, Marc [FR/FR]; 4, rue Viviane, F-14000
Caen (FR). TRAORE, Jacques [FR/FR]; 14, rue Emile
Dron, F-61100 Flers (FR).

(74) Mandataire : JEUNE, Pascale; France Telecom R &
D/VAT/VPI, 38-40, rue du Général Leclerc, F-92794 Issy
Moulineaux Cedex 9 (FR).

(81) États désignés (national) : AE, AG, AL, AM, AT, AU, AZ,
BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ,
DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM,
HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK,
LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX,
MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG,
SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC,
VN, YU, ZA, ZM, ZW.

(84) États désignés (régional) : brevet ARIPO (GH, GM, KE,
LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet
eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet
européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,
FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR),
brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW,
ML, MR, NE, SN, TD, TG).

Publiée :

- avec rapport de recherche internationale
- avant l'expiration du délai prévu pour la modification des
revendications, sera republiée si des modifications sont
reçues

En ce qui concerne les codes à deux lettres et autres abrévia-
tions, se référer aux "Notes explicatives relatives aux codes et
abréviations" figurant au début de chaque numéro ordinaire de
la Gazette du PCT.

(54) Title: CRYPTOGRAPHIC REVOCATION METHOD USING A CHIP CARD

(54) Titre : PROCEDE CRYPTOGRAPHIQUE DE REVOCATION A L'AIDE D'UNE CARTE A PUCE

(57) Abstract: The invention relates to a cryptographic method and to a chip card which is used to carry out said method. The inventive cryptographic method comprises the following steps: before any calculation is performed by a computing means of the chip card, said chip card reads (2) an integral list, in a storage means of a second entity, of identifiers of first proprietary entities of a chip card, said list being linked to each status assigned to each of the first entities by the second entity; and, subsequently, the chip card compares (3) the identifier stored in a storage means of the chip card with the contents of the list, in order to authorise (5) or prohibit (4) any calculation by the computing means depending the result of said comparison.

(57) Abrégé : La présente invention se rapporte à un procédé cryptographique et à une carte à puce pour la mise oeuvre du procédé. Le procédé cryptographique consiste avant tout calcul par un moyen de calcul de la carte à puce, à lire (2) par la carte à puce dans un moyen de mémorisation d'une seconde entité une liste d'identifiants sous forme intégrale de premières entités propriétaires d'une carte à puce, cette liste étant liée à chaque état attribué à chacune des premières entités par la seconde entité, à comparer (3), par la carte à puce, l'identifiant mémorisé dans un moyen de mémorisation de la carte à puce et le contenu de la liste, pour autoriser (5) ou interdire (4) tout calcul du moyen de calcul en fonction du résultat de la comparaison.



WO 03/060841 A1